We claim:

1. A system for performing cryptographic validity services, comprising:

a Distributed Storage Array comprising at least one Storage Device; and

a Distributed Processor Array coupled to the Distributed Storage Array, the Distributed Processor Array comprising at least one Processor, and the Distributed Storage Array storing a Program for controlling the Distributed Processor Array; and

the Distributed Processor Array is operative with the Program to

receive a Validation Request from a Relying Customer Interface;

formulate a Query responsive to the Validation Request;

transmit the Query to a Relying Participant Interface;

receive a Query Response from the Relying Participant Interface;

formulate a Validation Response responsive to the Query Response; and

transmit the Validation Response to the Relying Customer Interface.

2. The system for performing cryptographic validity services of Claim 1, wherein the Validation Response is further responsive to a Policy Engine.

3. The system for performing cryptographic validity services of Claim 1, wherein the Program comprises a Relying Customer Service Engine in communication with a Relying Participant Service Engine.

4. The system for performing cryptographic validity services of Claim 3, wherein the Distributed Processor Array is operative with the Relying Customer Service Engine to

receive the Validation Request from the Relying Customer Interface, and

transmit the Validation Response to the Relying Customer Interface; and

the Distributed Processor Array is operative with the Relying Participant Service Engine to

formulate the Query responsive to the Validation Request,

transmit the Query to the Relying Participant Interface,

receive the Query Response from the Relying Participant Interface, and

formulate the Validation Response responsive to the Query Response.

5. The system for performing cryptographic validity services of Claim 4, wherein the Distributed Processor Array is operative with the Relying Customer Service Engine to perform consistency checking on the Validation Request.

6. The system for performing cryptographic validity services of Claim 4, wherein the Distributed Processor Array is further operative with the Relying Customer Service Engine and the Distributed Processor Array is further operative with the Relying Participant Service Engine to establish a Communication Channel between the Relying Customer Service Engine and the Relying Participant Service Engine.

7. The system for performing cryptographic validity services of Claim 6, wherein the Communication Channel comprises the Internet.

8. The system for performing cryptographic validity services of Claim 6, wherein the Distributed Processor Array is further operative with the Relying Customer Service Engine to transmit the Validation Request to the Communication

Channel and receive the Validation Response from the Communication Channel; and the Distributed Processor Array is further operative with the Relying Participant Service Engine to receive the Validation Request from the Communication Channel and transmit the Validation Response to the Communication Channel.

9. The system for performing cryptographic validity services of Claim 8, wherein the Distributed Processor Array is further operative with the Relying Customer Service Engine to expose a System Application Programming Interface.

10. The system for performing cryptographic validity services of Claim 9, wherein configuration and control information for the Program is received through the System Application Programming Interface.

11. The system for performing cryptographic validity services of Claim 8, wherein the Distributed Processor Array is further operative with the Relying Customer Service Engine to expose an Information Application Programming Interface.

12. The system for performing cryptographic validity services of Claim 11, wherein the Relying Customer Interface comprises the Information Application Programming Interface.

13. The system for performing cryptographic validity services of Claim 12, wherein the Validation Request comprises an Electronic Signature, the Electronic Signature comprises a Digital Certificate and a Message Digest, wherein the Message Digest is responsive to Signed Data.

14. The system for performing cryptographic validity services of Claim 4, wherein the Relying Participant Service Engine comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

15. The system for performing cryptographic validity services of Claim 4, wherein the Distributed Processor Array is operative with the Relying Participant Service Engine to perform consistency checking on the Validation Request.

16. A system for performing cryptographic validity services, comprising:

a Distributed Storage Array comprising at least one Storage Device; and

a Distributed Processor Array coupled to the Distributed Storage Array, the Distributed Processor Array comprising at least one Processor, and the Distributed Storage Array storing a Program for controlling the Distributed Processor Array; and

the Distributed Processor Array is operative with the Program to

receive a Validation Request from a Communication Channel;

formulate a Query responsive to the Validation Request;

transmit the Query to a Relying Participant Interface;

receive a Query Response from the Relying Participant Interface;

formulate a Validation Response responsive to the Query Response; and

transmit the Validation Response to the Communication Channel.

17. The system for performing cryptographic validity services of Claim 16, wherein the Program comprises a Relying Participant Service Engine.

18. The system for performing cryptographic validity services of Claim 17, wherein the Relying Participant Service Engine comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

19. The system for performing cryptographic validity services of Claim 17, wherein the Distributed Processor Array is operative with the Relying Participant Service Engine to perform consistency checking on the Validation Request.

20. A method for performing cryptographic validity services, comprising:
receiving a Validation Request from a Relying Customer Interface;
formulating a Query responsive to the Validation Request;
transmitting the Query to a Relying Participant Interface;
receiving a Query Response from the Relying Participant Interface;
formulating a Validation Response responsive to the Query Response; and
transmitting the Validation Response to the Relying Customer Interface.

21. The method for performing cryptographic validity services of Claim 20, wherein the Validation Response is further responsive to a Policy Engine.

22. The method for performing cryptographic validity services of Claim 20, wherein receiving a Validation Request from a Relying Customer Interface and transmitting the Validation Request to the Relying Customer Interface are performed by a Relying Customer Service Engine; wherein formulating a Query responsive to the Validation Request, transmitting the Query to a Relying Participant Interface, receiving a Query Response from the Relying Participant Interface, and formulating a Validation Response responsive to the Query Response are performed by a Relying Participant Service Engine; and wherein the Relying Customer Service Engine is in communication with the Relying Participant Service Engine.

23. The method for performing cryptographic validity services of Claim 22, further comprising performing consistency checking on the Validation Request and

wherein performing consistency checking on the Validation Request is performed by the Relying Customer Service Engine.

24. The method for performing cryptographic validity services of Claim 22, further comprising establishing a Communication Channel between the Relying Customer Service Engine and the Relying Participant Service Engine.

25. The method for performing cryptographic validity services of Claim 24, wherein the Communication Channel comprises the Internet.

26. The method for performing cryptographic validity services of Claim 24, further comprising transmitting the Validation Request to the Communication Channel, receiving the Validation Response from the Communication Channel, receiving the Validation Request from the Communication Channel, and transmitting the Validation Response to the Communication Channel; wherein transmitting the Validation Request to the Communication Channel and receiving the Validation Response from the Communication Channel are performed by the Relying Customer Service Engine; and wherein receiving the Validation Request from the Communication Channel and transmitting the Validation Response to the Communication Channel are performed by the Relying Participant Service Engine.

27. The method for performing cryptographic validity services of Claim 26, further comprising exposing, by the Relying Customer Service Engine, a System Application Programming Interface.

28. The method for performing cryptographic validity services of Claim 27, further comprising receiving, by the Relying Customer Service Engine, configuration and control information through the System Application Programming Interface.

29. The method for performing cryptographic validity services of Claim 26, further comprising exposing, by the Relying Customer Service Engine, an Information Application Programming Interface.

30. The method for performing cryptographic validity services of Claim 29, wherein the Relying Customer Interface comprises the Information Application Programming Interface.

31. The method for performing cryptographic validity services of Claim 30, wherein the Validation Request comprises an Electronic Signature, the Electronic Signature comprising a Digital Certificate and a Message Digest, wherein the Message Digest is responsive to Signed Data.

32. The method for performing cryptographic validity services of Claim 22, wherein the Relying Participant Service Engine comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

33. The method for performing cryptographic validity services of Claim 22, further comprising performing, by the Relying Participant Service Engine, consistency checking on the Validation Request.

34. A method for performing cryptographic validity services, comprising:

receiving a Validation Request from a Communication Channel;

formulating a Query responsive to the Validation Request;

transmitting the Query to a Relying Participant Interface;

receiving a Query Response from the Relying Participant Interface;

formulating a Validation Response responsive to the Query Response; and

transmitting the Validation Response to the Communication Channel.

35. The method for performing cryptographic validity services of Claim 34, wherein receiving a Validation Request from a Communication Channel, formulating a Query responsive to the Validation Request, transmitting the Query to a Relying Participant Interface, receiving a Query Response from the Relying Participant Interface, formulating a Validation Response responsive to the Query Response, and transmitting the Validation Response to the Communication Channel are performed by a Relying Participant Service Engine.

36. The method for performing cryptographic validity services of Claim 35, wherein the Relying Participant Service Engine comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

37. The method for performing cryptographic validity services of Claim 35, further comprising performing, by the Relying Participant Service Engine, consistency checking on the Validation Request.

38. An apparatus for performing cryptographic validity services, comprising:

a Validation Request Receiver, wherein a Validation Request is received from a Relying Customer Interface;

a Query Formulator, in communication with the Validation Request Receiver, wherein a Query is formulated responsive to the Validation Request;

a Query Transmitter, in communication with the Query Formulator, wherein the Query is transmitted to a Relying Participant Interface;

a Query Response Receiver, wherein the Query Response is received

from the Relying Participant Interface;

a Validation Response Formulator, in communication with the Query Response Receiver, wherein a Validation Response is formulated responsive to the Query Response; and

a Validation Response Transmitter, in communication with the Validation Response Formulator, wherein the Validation Response is transmitted to the Relying Customer Interface.

39. The apparatus for performing cryptographic validity services of Claim 38, wherein the Validation Response Formulator comprises a Policy Engine, and the Validation Response is further responsive to the Policy Engine.

40. The apparatus for performing cryptographic validity services of Claim 38, further comprising a Relying Customer Service Engine in communication with a Relying Participant Service Engine, wherein the Relying Customer Service Engine comprises the Validation Request Receiver and the Validation Response Transmitter, and wherein the Relying Participant Service Engine comprises the Query Formulator, the Query Transmitter, the Query Response Receiver, and the Validation Response Formulator.

41. The apparatus for performing cryptographic validity services of Claim 40, wherein the Validation Request Receiver comprises a Consistency Checker and wherein the Consistency Checker performs consistency checking on the Validation Request.

42. The apparatus for performing cryptographic validity services of Claim 40, further comprising a Communication Channel in communication with the Relying

Customer Service Engine and in communication with the Relying Participant Service Engine.

43. The apparatus for performing cryptographic validity services of Claim 42, wherein the Communication Channel comprises the Internet.

44. The apparatus for performing cryptographic validity services of Claim 42, wherein the Validation Request Receiver transmits the Validation Request to the Communication Channel, the Query Formulator receives the Validation Request from the Communication Channel, the Validation Response Formulator transmits the Validation Response to the Communication Channel, and the Validation Response Transmitter receives the Validation Response from the Communication Channel.

45. The apparatus for performing cryptographic validity services of Claim 44, wherein the Relying Customer Service Engine exposes a System Application Programming Interface.

46. The apparatus for performing cryptographic validity services of Claim 45, wherein configuration and control information is received through the System Application Programming Interface.

47. The apparatus for performing cryptographic validity services of Claim 44, wherein the Relying Customer Service Engine exposes an Information Application Programming Interface.

48. The apparatus for performing cryptographic validity services of Claim 47, wherein the Relying Customer Interface comprises the Information Application Programming Interface.

49. The apparatus for performing cryptographic validity services of Claim 48, wherein the Validation Request comprises an Electronic Signature, the Electronic Signature comprising a Digital Certificate and a Message Digest, wherein the Message Digest is responsive to Signed Data.

50. The apparatus for performing cryptographic validity services of Claim 40, wherein the Validation Response Formulator comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

51. The apparatus for performing cryptographic validity services of Claim 40, wherein the Query Formulator comprises a Consistency Checker and wherein the Consistency Checker performs consistency checking on the Validation Request.

52. An apparatus for performing cryptographic validity services, comprising:

a Validation Request Receiver, wherein a Validation Request is received from a Communication Channel;

a Query Formulator, in communication with the Validation Request Receiver, wherein a Query is formulated responsive to the Validation Request;

a Query Transmitter, in communication with the Query Formulator, wherein the Query is transmitted to a Relying Participant Interface;

a Query Response Receiver, wherein the Query Response is received from the Relying Participant Interface;

a Validation Response Formulator, in communication with the Query Response Receiver, wherein a Validation Response is formulated responsive to the Query Response; and

a Validation Response Transmitter, in communication with the Validation

Response Formulator, wherein the Validation Response is transmitted to the Communication Channel.

53. The apparatus for performing cryptographic validity services of Claim 52, further comprising a Relying Participant Service Engine, wherein the Relying Participant Service Engine comprises the Validation Request Receiver, the Query Formulator, the Query Transmitter, the Query Response Receiver, the Validation Response Formulator, and the Validation Response Transmitter.

54. The apparatus for performing cryptographic validity services of Claim 53, wherein the Validation Response Formulator comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

55. The apparatus for performing cryptographic validity services of Claim 54, wherein the Query Formulator comprises a Consistency Checker and wherein the Consistency Checker performs consistency checking on the Validation Request.

56. An apparatus for performing cryptographic validity services, comprising:

means for receiving a Validation Request from a Relying Customer Interface;

means, in communication with the means for receiving a Validation Request from a Relying Customer Interface, for formulating, responsive to the Validation Request, a Query;

means, in communication with the means for formulating a Query, for transmitting the Query to a Relying Participant Interface;

means for receiving a Query Response from the Relying Participant Interface;

means, in communication with the means for receiving a Query Response

from the Relying Participant Interface, for formulating, responsive to the Query Response, a Validation Response; and

means, in communication with the means for formulating a Validation Response, for transmitting the Validation Response to the Relying Customer Interface.

57. The apparatus for performing cryptographic validity services of Claim 56, wherein the means for formulating a Validation Response comprises a Policy Engine, and the Validation Response is further responsive to the Policy Engine.

58. The apparatus for performing cryptographic validity services of Claim 56, further comprising a Relying Customer Service Engine in communication with a Relying Participant Service Engine, wherein the Relying Customer Service Engine comprises the means for receiving a Validation Request from a Relying Customer Interface and the means for transmitting the Validation Response to the Relying Customer Interface, and wherein the Relying Participant Service Engine comprises the means for formulating a Query, the means for transmitting the Query to the Relying Participant Interface, the means for receiving a Query Response from the Relying Participant Interface, and the means for formulating a Validation Response.

59. The apparatus for performing cryptographic validity services of Claim 58, wherein the means for receiving a Validation Request from a Relying Customer Interface comprises means for performing consistency checking on the Validation Request.

60. The apparatus for performing cryptographic validity services of Claim 58, further comprising a Communication Channel in communication with the Relying

Customer Service Engine and in communication with the Relying Participant Service Engine.

61. The apparatus for performing cryptographic validity services of Claim 60, wherein the Communication Channel comprises the Internet.

62. The apparatus for performing cryptographic validity services of Claim 60, wherein the means for receiving a Validation Request from a Relying Customer Interface comprises means for transmitting the Validation Request to the Communication Channel, the means for formulating a Query comprises means for receiving the Validation Request from the Communication Channel, the means for formulating a Validation Response comprises means for transmitting the Validation Response to the Communication Channel, and the means for transmitting the Validation Response to the Relying Customer Interface comprises means for receiving the Validation Response from the Communication Channel.

63. The apparatus for performing cryptographic validity services of Claim 62, wherein the Relying Customer Service Engine further comprises means for exposing a System Application Programming Interface.

64. The apparatus for performing cryptographic validity services of Claim 63, wherein configuration and control information is received through the System Application Programming Interface.

65. The apparatus for performing cryptographic validity services of Claim 62, wherein the Relying Customer Service Engine has means for exposing an Information Application Programming Interface.

66. The apparatus for performing cryptographic validity services of Claim 65, wherein the Relying Customer Interface comprises the Information Application Programming Interface.

67. The apparatus for performing cryptographic validity services of Claim 66, wherein the Validation Request comprises an Electronic Signature, the Electronic Signature comprising a Digital Certificate and a Message Digest, wherein the Message Digest is responsive to Signed Data.

68. The apparatus for performing cryptographic validity services of Claim 58, wherein the means for formulating a Validation Response comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

69. The apparatus for performing cryptographic validity services of Claim 58, wherein the means for formulating a Query comprises means for performing consistency checking on the Validation Response.

70. An apparatus for performing cryptographic validity services, comprising:

means for receiving a Validation Request from a Communication Channel;

means, in communication with the means for receiving a Validation Request from a Communication Channel, for formulating, responsive to the Validation Request, a Query;

means, in communication with the means for formulating a Query, for transmitting the Query to a Relying Participant Interface;

means for receiving a Query Response from the Relying Participant Interface;

means, in communication with the means for receiving a Query Response

from the Relying Participant Interface, for formulating, responsive to the Query Response, a Validation Response; and

means, in communication with the means for formulating a Validation Response, for transmitting the Validation Response to the Communication Channel.

71. The apparatus for performing cryptographic validity services of Claim 70, further comprising a Relying Participant Service Engine, wherein the Relying Participant Service Engine comprises the means for receiving a Validation Request from a Communication Channel, the means for formulating a Query, the means for transmitting the Query to the Relying Participant Interface, the means for receiving a Query Response from the Relying Participant Interface, the means for formulating a Validation Response, and the means for transmitting the Validation Response to the Communication Channel.

72. The apparatus for performing cryptographic validity services of Claim 71, wherein the means for formulating a Validation Response comprises a Policy Engine and the Validation Response is further responsive to the Policy Engine.

73. The apparatus for performing cryptographic validity services of Claim 72, wherein the means for formulating a Query comprises means for performing consistency checking on the Validation Request.